PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-052134
(43)Date of publication of application : 23.02.2001

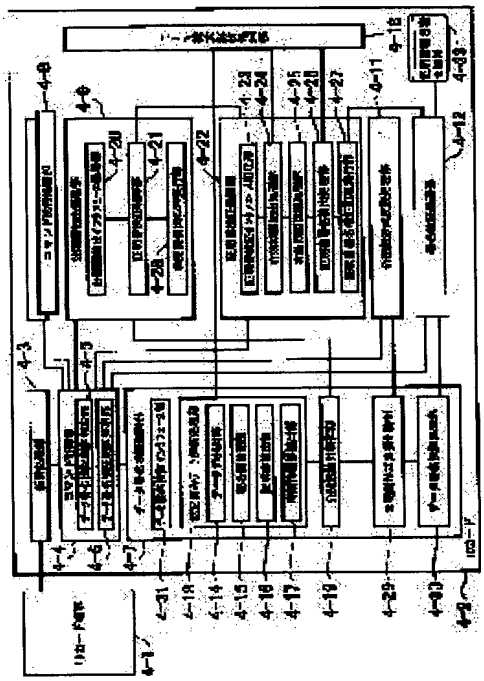
(51)Int.CI. G06K 19/073
G06K 17/00
G09C 1/00

(21)Application number : 11-221537
(22)Date of filing : 04.08.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NIWANO EIICHI
SUZUKI KATSUHIKO
CHIBA NOBUHIRO
HOSODA YASUHIRO

(54) METHOD AND DEVICE FOR PROCESSING IC CARD SYSTEM COMMUNICATION DATA PROTECTION AND RECORDING MEDIUM RECORDING IC CARD SYSTEM COMMUNICATION DATA PROTECTION PROCESSING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a device for processing IC card system communication data protection and a recording medium recording IC card system communication data protection processing program with which revising or illegality of data transferred to an IC card in a distributed environment including the IC card is prevented and data can be safely distributed.
SOLUTION: This device is provided with a data part transmitted from an IC card terminal 4-1, a signature using the secret key of a person to prove this data part, the identifier of the owner of a public key for proving the public key in respect to the secret key used for this signature, the public key of a data part signer, the identifier and signature of a verification institution for guaranteeing these identifier and the public key information at least, further, the public key is extracted from a certificate on the basis of the certificate containing the limit of the validity of this proof and signature verifying processing is executed on the basis of this extracted public key.



LEGAL STATUS

[Date of request for examination] 06.11.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－52134
（P2001－52134A）
(43)公開日　平成13年２月23日(2001.2.23)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
G06K 19/073		G06K 19/00	P	5B035
17/00			17/00	E	5B058
G09C 1/00	640	G09C 1/00	640B	5J104
			640Z	
	660		660A	

審査請求　未請求　請求項の数24　ＯＬ　（全 21 頁）

(21)出願番号　特願平11－221537

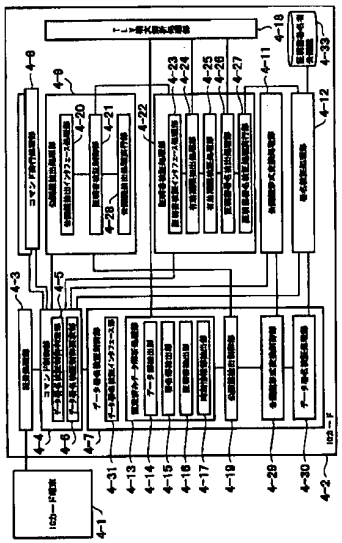
(22)出願日　平成11年８月４日(1999.8.4)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　庭野　栄一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　鈴木　勝彦
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　ＩＣカードシステム通信データ保護処理方法および装置とＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体

(57)【要約】
【課題】　ＩＣカードを含む分散環境においてＩＣカードに転送されたデータの改竄または不正を防止し、データを安全に流通させることができるＩＣカードシステム通信データ保護処理方法および装置とＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体を提供する。
【解決手段】　ＩＣカード端末４－１から送信されたデータ部、このデータ部を保証する人の秘密鍵を用いた署名、この署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書に基づき証明書から公開鍵を抽出し、この抽出された公開鍵に基づいて署名検証処理を実行する。



【特許請求の範囲】
【請求項１】　ＩＣカードサービスサーバと、ＩＣカード端末と、該ＩＣカード端末とＩＣカードの通信を行う転送処理手段、ＩＣカード端末から送信または要求されるコマンドデータを所望のコマンド実行部にディスパッチするためのコマンド制御手段、およびコマンドを実行する複数のコマンド実行手段を有するＩＣカードとを有するＩＣカードシステムにおいてＩＣカードサービスサーバからＩＣカード端末を介してまたはＩＣカード端末からＩＣカードに送信されたデータの改竄または不正を防止するためのＩＣカードシステム通信データ保護処理方法であって、
ＩＣカードにおいては、ＩＣカード端末から送信されたデータ部、このデータ部を保証する人の秘密鍵を用いた署名、この署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書に基づき証明書から公開鍵を抽出する公開鍵抽出処理と、
この抽出された公開鍵に基づいて署名検証処理を実行するデータ署名検証処理を少なくとも有するデータ署名検証制御処理とを行うことを特徴とするＩＣカードシステム通信データ保護処理方法。
【請求項２】　データ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータが前記ＩＣカード端末からＩＣカードに送信され、
前記データ署名検証制御処理においては、ＩＣカード端末から送信されたデータ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出処理、署名部抽出処理、および証明書抽出処理で構成される認定済みデータ解析処理を行うことを特徴とする請求項１記載のＩＣカードシステム通信データ保護処理方法。
【請求項３】　前記公開鍵抽出処理においては、証明書検証処理内で証明書内の認証機関の署名を検証する証明書署名検証処理を行うことを特徴とする請求項１または２記載のＩＣカードシステム通信データ保護処理方法。
【請求項４】　前記データ解析処理においてはＩＣカード端末から付加的な要素として送信された時刻に基づき、前記証明書検証処理において証明書から有効期限を抽出する有効期限抽出処理と、前記ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理とを行うことを特徴とする請求項１または３記載のＩＣカードシステム通信データ保護処理方法。
【請求項５】　前記データ解析処理においては、前記ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離する時刻情報抽出処理を行い、
前記証明書検証処理においては、証明書から有効期限を抽出する有効期限抽出処理と、前記時刻情報抽出処理で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理を行うことを特徴とする請求項２または３記載のＩＣカードシステム通信データ保護処理方法。
【請求項６】　前記証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、前記ＩＣカードにおいては、認定済みデータ解析処理または有効期限抽出処理または証明書署名抽出処理から要求を受け付け、前記バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理を行うことを特徴とする請求項３または４または５記載のＩＣカードシステム通信データ保護処理方法。
【請求項７】　前記コマンド制御処理においては、ＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定処理と、コマンド実行処理にディスパッチする前に、前記データ署名検証制御判定処理の結果に基づき署名・証明書がある場合にデータ署名検証制御処理に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御処理とを行うことを特徴とする請求項１乃至６のいずれかに記載のＩＣカードシステム通信データ保護処理方法。
【請求項８】　前記データ署名検証制御処理においては、前記ＩＣカード端末からの要求を受け、コマンドの制御処理から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御に返却するデータ署名検証インタフェース処理を行い、
前記公開鍵抽出処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御処理に返却する公開鍵抽出インタフェース処理を行い、
前記証明　検証処理においては、前記ＩＣカード端末か

らの要求を受け、コマンド制御処理から証明書と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明書の正当性の検証結果をコマンド制御処理に返却する証明書検証インタフェース処理を行うことを特徴とする請求項１乃至７のいずれかに記載のＩＣカードシステム通信データ保護処理方法。

【請求項９】　ＩＣカードサービスサーバと、ＩＣカード端末と、該ＩＣカード端末とＩＣカードの通信を行う転送処理手段、ＩＣカード端末から送信または要求されるコマンドデータを所望のコマンド実行部にディスパッチするためのコマンド制御手段、およびコマンドを実行する複数のコマンド実行手段を有するＩＣカードとを有するＩＣカードシステムにおいてＩＣカードサービスサーバからＩＣカード端末を介してまたはＩＣカード端末からＩＣカードに送信されたデータの改竄または不正を防止するためのＩＣカードシステム通信データ保護処理装置であって、

ＩＣカードは、ＩＣカード端末から送信されたデータ部、このデータ部を保証する人の秘密鍵を用いた署名、この署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書に基づき証明書から公開鍵を抽出する公開鍵抽出処理手段と、

この抽出された公開鍵に基づいて署名検証処理を実行するデータ署名検証処理手段を少なくとも有するデータ署名検証制御手段とを有することを特徴とするＩＣカードシステム通信データ保護処理装置。

【請求項１０】　データ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータが前記ＩＣカード端末からＩＣカードに送信され、

前記データ署名検証制御手段は、ＩＣカード端末から送信されたデータ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出手段、署名部抽出手段、および証明書抽出手段で構成される認定済みデータ解析処理手段を有することを特徴とする請求項９記載のＩＣカードシステム通信データ保護処理装置。

【請求項１１】　前記公開鍵抽出処理手段は、証明書検証処理手段内に証明書内の認証機関の署名を検証する証明書署名検証処理手段を有することを特徴とする請求項９または１０記載のＩＣカードシステム通信データ保護処理装置。

【請求項１２】　前記証明書検証処理手段は、証明書から有効期限を抽出する有効期限抽出処理手段と、前記ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と前記有効期限抽出手段で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理手段とを有することを特徴とする請求項９または１１記載のＩＣカードシステム通信データ保護処理装置。

【請求項１３】　前記データ解析手段は、前記ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離する時刻情報抽出処理手段を有し、

前記証明書検証処理手段は、証明書から有効期限を抽出する有効期限抽出処理手段と、前記時刻情報抽出手段で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と前記有効期限抽出手段で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理手段を有することを特徴とする請求項１０または１１記載のＩＣカードシステム通信データ保護処理装置。

【請求項１４】　前記証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、前記ＩＣカードは、認定済みデータ解析処理手段または有効期限抽出処理手段または証明書署名抽出処理手段から要求を受け付け、前記バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理手段を有することを特徴とする請求項１１または１２または１３記載のＩＣカードシステム通信データ保護処理装置。

【請求項１５】　前記コマンド制御手段は、ＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定手段と、コマンド実行手段にディスパッチする前に、前記データ署名検証制御判定手段の結果に基づき署名・証明書がある場合にデータ署名検証制御手段に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御手段とを有することを特徴とする請求項９乃至１４のいずれかに記載のＩＣカードシステム通信データ保護処理装置。

【請求項１６】　前記データ署名検証制御手段は、前記ＩＣカード端末からの要求を受け、コマンドの制御手段から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御手段に返却するデータ署名検証インタフェース手段を有し、

前記公開鍵抽出処理手段は、前記ＩＣカード端末からの要求を受け、コマンド制御手段から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御手段に返却する公開鍵抽出インタフェース処理手段を有し、

前記証明書検証処理手段は、前記ＩＣカード端末からの要求を受け、コマンド制御手段から証明書と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明書の正当性の検証結果をコマンド制御手段に返却する証明書検証インタフェース手段を有することを特徴とする請求項９乃至１５のいずれかに記載のＩＣカードシステム通信データ保護処理装置。

【請求項１７】　ＩＣカードサービスサーバと、ＩＣカード端末と、該ＩＣカード端末とＩＣカードの通信を行う転送処理手段、ＩＣカード端末から送信または要求されるコマンドデータを所望のコマンド実行部にディスパッチするためのコマンド制御手段、およびコマンドを実行する複数のコマンド実行手段を有するＩＣカードとを有するＩＣカードシステムにおいてＩＣカードサービスサーバからＩＣカード端末を介してまたはＩＣカード端末からＩＣカードに送信されたデータの改竄または不正を防止するためのＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体であって、

ＩＣカードにおいては、ＩＣカード端末から送信されたデータ部、このデータ部を保証する人の秘密鍵を用いた署名、この署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書に基づき証明書から公開鍵を抽出する公開鍵抽出処理と、

この抽出された公開鍵に基づいて署名検証処理を実行するデータ署名検証処理を少なくとも有するデータ署名検証制御処理とを行うことを特徴とするＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体。

【請求項１８】　データ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータが前記ＩＣカード端末からＩＣカードに送信され、

前記データ署名検証制御処理においては、ＩＣカード端末から送信されたデータ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出処理、署名部抽出処理、および証明書抽出処理で構成される認定済みデータ解析処理を行うことを特徴とする請求項１７記載のＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体。

【請求項１９】　前記公開鍵抽出処理においては、証明書検証処理内に証明書内の認証機関の署名を検証する証明書署名検証処理を行うことを特徴とする請求項１７または１８記載のＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体。

【請求項２０】　前記データ解析処理においてはＩＣカード端末から付加的な要素として送信された時刻に基づき、前記証明書検証処理において証明書から有効期限を抽出する有効期限抽出処理と、前記ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理とを行うことを特徴とする請求項１７または１９記載のＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体。

【請求項２１】　前記データ解析処理においては、前記ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離する時刻情報抽出処理を行い、

前記証明書検証処理においては、証明書から有効期限を抽出する有効期限抽出処理と、前記時刻情報抽出処理で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理を行うことを特徴とする請求項１８または１９記載のＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体。

【請求項２２】　前記証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、前記ＩＣカードにおいては、前記認定済みデータ解析処理または前記有効期限抽出処理または証明書署名抽出処理から要求を受け付け、前記バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理を行うことを特徴とする請求項１９または２０または２１記載のＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体。

【請求項２３】　前記コマンド制御処理においては、ＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定処理と、コマンド実行処理にディスパッチする前に、前記データ署名検証制御判定処理の結果に基づき署名・証明書がある場合にデータ署名検証制御処理に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御処理とを行うことを特徴とする請求項１７乃至２２のいずれかに記載のＩＣカードシステム通信データ保護処理プログラムを記

録した記録媒体。

【請求項２４】　前記データ署名検証制御処理においては、前記ＩＣカード端末からの要求を受け、コマンドの制御処理から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御処理に返却するデータ署名検証インタフェース処理を行い、
前記公開鍵抽出処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御処理に返却する公開鍵抽出インタフェース処理を行い、
前記証明書検証処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から証明書と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明書の正当性の検証結果をコマンド制御処理に返却する証明書検証インタフェース処理を行うことを特徴とする請求項１７乃至２３のいずれかに記載のＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数のＩＣカードサーバ、ＩＣカード端末、ＩＣカード間を含んだ分散環境においてアプリケーションプログラムまたは任意のデータを流通させるような分散ＩＣカードシステムにおいてＩＣカードサーバからＩＣカード端末を介してＩＣカードにまたはＩＣカード端末からＩＣカードに送信されたデータの改竄または不正を防止するためのＩＣカードシステム通信データ保護処理方法および装置とＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】ＩＳＯ／ＪＩＣＳＡＰにおいては、ＩＣカード端末からＩＣカードへのデータの送信時のデータ保護に関する方式としてセキュアメッセージングと呼ばれる暗号化方法が提案されている。しかしながら、ＩＣカード端末とＩＣカード間でのデータの改竄検出に関する規定は特にない。従って、アプリケーションダウンロード時のアプリケーションの改竄あるいは不正を防止するための規定は行っていない。

【０００３】ＪａｖａＣａｒｄにおいては、プログラムダウンロード時のプログラムの改竄あるいは不正なプログラムの介入を防止するために、プログラムデータに対して秘密鍵により署名を施し、この署名検証を端末において実施してからＩＣカード内に転送する方式が開示されている。

【０００４】また、ＭｕｌｔｏｓにおいてはＪａｖａＣａｒｄと異なりプログラムに対する署名の検証はＩＣカード内部において実施する。次に、図４に示す従来のＩＣカード通信データ保護処理方法を実施するＩＣカードシステムのモジュール構成図を参照して、簡単に手順を説明する。

【０００５】まず最初に、Open MEL Applicationコマンドを実行し、領域の確保を行う。次に、LoadCodeコマンドによるプログラムデータのダウンロード（図４のプログラムダウンロード処理部１－１）やLodeApplicationSignatureコマンドによるアプリケーションへの署名データのダウンロード（図４の署名ダウンロード処理部１－２）を行った後、CreateMELApplicationコマンドによるアプリケーションの生成（図４のアプリケーション生成処理部１－３）時に、ＡＬＣと呼ばれるＭｕｌｔｏｓ独自の証明書データをダウンロード（図４の独自証明書ダウンロード処理部１－４）し、この中に含まれる該署名データの秘密鍵に対する公開鍵を、独自の証明書形式に対する構文解析（図４の独自構文解析処理部１－５）を実施して、抽出（図４の公開鍵抽出処理部１－６）した後、署名の検証（図４の署名検証処理部１－７）を行うという方法である。

【０００６】これらのコマンドはＩＣカード端末１－８からＩＣカード１－９への伝送制御を実施する転送処理部１－１０を介して、コマンド制御部１－１１が該プログラムダウンロードコマンド、署名ダウンロードコマンド、アプリケーション生成処理コマンドなどの所望のコマンドのコマンド実行処理部１－１２にディスパッチすることによって実施される。

【０００７】

【発明が解決しようとする課題】上述した従来方法では、まず、ＪａｖａＣａｒｄに対しては以下のような問題がある。

【０００８】（１－ａ）ＪａｖａＣａｒｄにおいては、署名の検証を端末で実行するために、プログラムをＩＣカード内に転送する際に、改竄の恐れがあり、またプログラムを実行する装置上で検証が実施されないために、端末が信用できない場合にはセキュリティ上の不安がある。

【０００９】またＭｕｌｔｏｓはこの問題を解決し、ＩＣカード内で認証処理を実行する方式を提案している。すなわち、Ｍｕｌｔｏｓにおいては、ＩＣカード発行者の管理機関において、ＩＣカードプログラムおよびＩＣカード発行期間を管理し、ＩＣカードのダウンロードをＩＣカード発行者およびＩＣカード発行者より認定された機関に限定するなど、プログラムのダウンロード（流通）を特定の機関に制限することによってプログラム改竄に対する脅威を防御・データ保証（プログラム保証）している。

【００１０】しかしながら、現状のようなインターネットを始めとする分散環境においては、情報流通を促進させるためにはアプリケーションプロバイダ（プログラムの提供者）をＩＣカードを提供するサービスプロバイダまで柔軟に拡大し、かつエンドユーザ間でも自由にプログラムを交換できるようなオープンな環境が望まれる。また、更にプログラムだけではなく一般のデータに対しても署名・証明書付きで分散流通が図れるような環境の提供が望ましい。従って、このような環境を安全に提供することが重要である。

【００１１】以下ではこのような分散流通環境に対して、Ｍｕｌｔｏｓ方式を適応しようとする場合の課題について説明する。

【００１２】（１－ｂ）Ｍｕｌｔｏｓにおいては証明書形式が独自であるため分散環境において流通させた場合に、Ｍｕｌｔｏｓ環境以外との相互運用ができない。すなわち、例えば一般に流通しているＸ．５０９の証明書を用いた署名を施したデータをそのままＩＣカード内で処理することができない。

【００１３】（１－ｃ）Ｍｕｌｔｏｓにおいては管理機関とＩＣカードダウンロード実行者間のプログラムダウンロードを想定しているため、管理機関とＩＣカードダウンロード実行者（ＩＣカード発行機関）の間で証明書をＩＣカード発行機関の公開鍵に基づく暗号処理によって安全に送信することが可能であるが、プログラムデータをエンドユーザ間で柔軟に流通させるような環境を提供する際には、署名と証明書をともに流通させる必要がある。しかしながら、このような分散ＩＣカードシステム環境に対してＭｕｌｔｏｓ方式を適応すると証明書に対する認定機関の署名がないために証明書が途中で改竄される恐れがある。

【００１４】（１－ｄ）Ｍｕｌｔｏｓでは前述のように、ＩＣカードの発行者（あるいはＩＣカード発行者から認定されたビューロと呼ばれるアプリケーションダウンロードが可能な機関）が管理機関により管理されており、かつ常に、アプリケーションダウンロード時には管理機関に対してプログラムのダウンロードと証明書の転送が実行されるため、証明書に対する有効期間が設定されていなくても問題ないが、これを前述のようなアプリケーションをエンドユーザ間で柔軟に開発、流通させるような分散ＩＣカードシステム環境においては、証明書のエンドユーザ間での流通が生じてくるため、公開鍵所有者に対する保証期間を設定するためなどの目的で証明書に対する有効期間を知ることができなくてはならない。

【００１５】（２）Ｍｕｌｔｏｓにおいてはアプリケーション、署名、証明書の管理者が特定の機関であり、かつアプリケーションダウンロード時には必ずこの管理機関からダウンロードするため、アプリケーション、署名、証明書が分散されてダウンロードされても問題がないが、プログラムデータをエンドユーザ間で柔軟に流通させるような環境を提供する際には、プログラム、署名、証明書は一体で管理した方が流通による紛失を避けるためあるいは処理の容易性を確保する上でも望ましい。

【００１６】（３）上記（１－ｃ）で指摘したように、Ｍｕｌｔｏｓにおいては認定機関による証明書への署名がなく、従ってこの署名を検証する手段が提供されていないため署名検証が実施できない。

【００１７】（４）（１）の条件下において、上記（１－ｄ）で指摘したような有効期間を検証する場合には、現状ＩＣカード内部では時刻情報を管理することが難しいため、時刻情報管理機能がついていないＩＣカードにおいては、時刻情報を知ることができない。また知ったとしてもこの時刻情報と有効期間を比較検証する手段が提供されていない。

【００１８】（５）（２）の条件下において、上記（１－ｄ）で指摘したような有効期間を検証する場合には、一体化されたプログラム・署名・証明書とともに時刻情報をコマンドで送信する必要があるが、この場合に証明書の有効期間を検証する際に送信されたデータの中から時刻情報を分離する必要とこの時刻情報と有効期間を比較検証する手段を提供する必要がある。

【００１９】（６）従来のタグ・レングス・値の構造をもつ例えばＸ．５０９のような証明書を処理する場合には一般に、タグ・レングス・値の構造をもつバイナリデータ（ＡＳＮ．１転送構文：ＴＬＶ構造データ）からＡＳＮ．１コンパイラを介して例えばＣの構造体に変換した後、必要な構造体のメンバを参照するような方式が取られていた。しかしながら、ＩＣカードのようにメモリ資源が少ない装置においては、ＡＳＭ．１コンパイラを登載して処理することは難しく簡易な処理方式が望まれている。

【００２０】（７）Ｍｕｌｔｏｓについてはアプリケーションに対するダウンロードに関しては、データの改竄・不正に対する保護方法を署名・証明書を用いた方式として規定しているが一般のデータに対しては規定を行っていない。従って、これを一般のデータへと拡張し、書き込みコマンドを始めとする任意のコマンドの改竄・不正を防止する仕組みが必要である。

【００２１】（８）Ｍｕｌｔｏｓにおいては証明書を処理するためのインタフェースが端末側に公開されていないために端末側で簡単にＩＣカードを利用した証明書処理が実施できない。

【００２２】本発明は、上記に鑑みてなされたもので、その目的とするところは、ＩＣカードを含む分散環境においてＩＣカードに転送されたデータの改竄または不正を防止し、データを安全に流通させることができるＩＣカードシステム通信データ保護処理方法および装置とＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体を提供することにある。

【００２３】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、ＩＣカードサービスサーバと、ＩＣカード端末と、該ＩＣカード端末とＩＣカー

ドの通信を行う転送処理手段、ＩＣカード端末から送信または要求されるコマンドデータを所望のコマンド実行部にディスパッチするためのコマンド制御手段、およびコマンドを実行する複数のコマンド実行手段を有するＩＣカードとを有するＩＣカードシステムにおいてＩＣカードサービスサーバからＩＣカード端末を介してまたはＩＣカード端末からＩＣカードに送信されたデータの改竄または不正を防止するためのＩＣカードシステム通信データ保護処理方法であって、ＩＣカードにおいては、ＩＣカード端末から送信されたデータ部、このデータ部を保証する人の秘密鍵を用いた署名、この署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書に基づき証明書から公開鍵を抽出する公開鍵抽出処理と、この抽出された公開鍵に基づいて署名検証処理を実行するデータ署名検証処理を少なくとも有するデータ署名検証制御処理とを行うことを要旨とする。

【００２４】請求項１記載の本発明にあっては、証明書から公開鍵を抽出し、この抽出された公開鍵に基づいて署名検証処理を実行するため、プログラムまたはデータに対する署名検証をＩＣカード内で実施することができ、また公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書形式を処理するため、既存に流通している証明書と整合性の高い署名検証処理が可能となり、また認証機関の署名と証明書有効期間が設定されているため、この情報を利用すれば証明書を流通させても改竄の恐れがなく、また証明書が有効でない場合に利用するという危険を回避することが可能となる。

【００２５】また、請求項２記載の本発明は、請求項１記載の発明において、データ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータが前記ＩＣカード端末からＩＣカードに送信され、前記データ署名検証制御処理においては、ＩＣカード端末から送信されたデータ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出処理、署名部抽出処理、および証明書抽出処理で構成される認定済みデータ解析処理を行うことを要旨とする。

【００２６】請求項２記載の本発明にあっては、データ署名検証制御処理において公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出処理、署名部抽出処理、および証明書抽出処理を行うため、データ、署名、証明書が一体となったデータ（ファイル）として管理可能であり、分散環境において署名・証明書付きデータを流通させた場合に、個々に管理する場合に比較して、紛失することを避けやすくなるなど管理上の混乱を避けることが可能となるとともに、処理の容易性も確保できる。

【００２７】更に、請求項３記載の本発明は、請求項１または２記載の発明において、前記公開鍵抽出処理においては、証明書検証処理内で証明書内の認証機関の署名を検証する証明書署名検証処理を行うことを要旨とする。

【００２８】請求項３記載の本発明にあっては、公開鍵抽出処理においては証明書検証処理内で証明書内の認証機関の署名を検証するため、証明書に対する認証機関の証明書検証処理が実際に可能となり、証明書の有効性の有無を確認し、不当なプログラムまたはデータの利用を回避することができる。

【００２９】請求項４記載の本発明は、請求項１または３記載の発明において、前記データ解析処理においてはＩＣカード端末から付加的な要素として送信された時刻に基づき、前記証明書検証処理において証明書から有効期限を抽出する有効期限抽出処理と、前記ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理とを行うことを要旨とする。

【００３０】請求項４記載の本発明にあっては、ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行うため、証明書の有効期間の検証処理を行うことができる。

【００３１】また、請求項５記載の本発明は、請求項２または３記載の発明において、前記データ解析処理においては、前記ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離する時刻情報抽出処理を行い、前記証明書検証処理においては、証明書から有効期限を抽出する有効期限抽出処理と、前記時刻情報抽出処理で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理を行うことを要旨とする。

【００３２】請求項５記載の本発明にあっては、ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離し、証明書から有効期限を抽出し、時刻情報抽出処理で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行うため、ＩＣカード端末から送信されたデータの中から時刻情報を抽出することができ、この時刻情報に基づいて証明書の有効期間の検証が可能となる。

【００３３】更に、請求項６記載の本発明は、請求項３または４または５記載の発明において、前記証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、前記ＩＣカードにおいては、認定済みデータ解析処理または有効期限抽出処理または証明書署名抽出処理から要求を受け付け、前記バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理を行うことを要旨とする。

【００３４】請求項６記載の本発明にあっては、証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、認定済みデータ解析処理または有効期限抽出処理または証明書署名抽出処理から要求を受け付け、バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理を行うため、従来のタグ、レングス、値の構造（以下、ＴＬＶ構造と称する）を有する例えばＸ．５０９の転送構文データをＩＣカード内で処理する場合に、高速にＩＣカード内で証明書から有効期限抽出処理または公開鍵抽出処理を行うことができる。

【００３５】請求項７記載の本発明は、請求項１乃至６のいずれかに記載の発明において、前記コマンド制御処理においては、ＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定処理と、コマンド実行処理にディスパッチする前に、前記データ署名検証制御判定処理の結果に基づき署名・証明書がある場合にデータ署名検証制御処理に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御処理とを行うことを要旨とする。

【００３６】請求項７記載の本発明にあっては、コマンド制御処理においてはＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定処理と、コマンド実行処理にディスパッチする前に、データ署名検証制御判定処理の結果に基づき署名・証明書がある場合にデータ署名検証制御処理に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御処理とを行うため、ダウンロードコマンド以外の任意のコマンドに対してコマンドの実行前にコマンドに対して入力されたデータに対して署名の検証処理を実行し、データの正当性を検証することができる。

【００３７】また、請求項８記載の本発明は、請求項１乃至７のいずれかに記載の発明において、前記データ署名検証制御処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御に返却するデータ署名検証インタフェース処理を行い、前記公開鍵抽出処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御処理に返却する公開鍵抽出インタフェース処理を行い、前記証明書検証処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から証明と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明書の正当性の検証結果をコマンド制御処理に返却する証明書検証インタフェース処理を行うことを要旨とする。

【００３８】請求項８記載の本発明にあっては、データ署名検証制御処理においてＩＣカード端末からの要求を受け、コマンドの制御処理から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御に返却するデータ署名検証インタフェース処理を行い、公開鍵抽出処理においてはＩＣカード端末からの要求を受け、コマンド制御処理から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御処理に返却する公開鍵抽出インタフェース処理を行い、証明検証処理においてはＩＣカード端末からの要求を受け、コマンド制御処理から証明書と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明　の正当性の検証結果をコマンド制御処理に返却する証明書検証インタフェース処理を行うため、例えば端末側から簡単に例えばＸ．５０９の証明書形式を有する証明書に対するＩＣカードを利用した多様な証明書処理を実施することができる。

【００３９】更に、請求項９記載の本発明は、ＩＣカードサービスサーバと、ＩＣカード端末と、該ＩＣカード端末とＩＣカードの通信を行う転送処理手段、ＩＣカード端末から送信または要求されるコマンドデータを所望のコマンド実行部にディスパッチするためのコマンド制御手段、およびコマンドを実行する複数のコマンド実行手段を有するＩＣカードとを有するＩＣカードシステムにおいてＩＣカードサービスサーバからＩＣカード端末を介してまたはＩＣカード端末からＩＣカードに送信さ

れたデータの改竄または不正を防止するためのＩＣカードシステム通信データ保護処理装置であって、ＩＣカードは、ＩＣカード端末から送信されたデータ部、このデータ部を保証する人の秘密鍵を用いた署名、この署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明　に基づき証明書から公開鍵を抽出する公開鍵抽出処理手段と、この抽出された公開鍵に基づいて署名検証処理を実行するデータ署名検証処理手段を少なくとも有することを要旨とする。

【００４０】請求項９記載の本発明にあっては、証明書から公開鍵を抽出し、この抽出された公開鍵に基づいて署名検証処理を実行するため、プログラムまたはデータに対する署名検証をＩＣカード内で実施することができ、また公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書形式を処理するため、既存に流通している証明書と整合性の高い署名検証処理が可能となり、また認証機関の署名と証明書有効期間が設定されているため、この情報を利用すれば証明書を流通させても改竄の恐れがなく、また証明書が有効でない場合に利用するという危険を回避することが可能となる。

【００４１】請求項１０記載の本発明は、請求項９記載の発明において、データ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータが前記ＩＣカード端末からＩＣカードに送信され、前記データ署名検証制御手段が、ＩＣカード端末から送信されたデータ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出手段、署名部抽出手段、および証明書抽出手段で構成される認定済みデータ解析処理手段を有することを要旨とする。

【００４２】請求項１０記載の本発明にあっては、データ署名検証制御処理において公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明　部で少なくとも構成される認定済みデータの解析を行うデータ抽出処理、署名部抽出処理、および証明書抽出処理を行うため、データ、署名、証明書が一体となったデータ（ファイル）として管理可能であり、分散環境において署名・証明書付きデータを流通せた場合に、個々に管理する場合に比較して、紛失することを避けやすくなるなど管理上の混乱を避けることが可能となるとともに、処理の容易性も確保できる。

【００４３】また、請求項１１記載の本発明は、請求項９または１０記載の発明において、前記公開鍵抽出処理手段が、証明書検証処理手段内に証明書内の認証機関の署名を検証する証明書署名検証処理手段を有することを要旨とする。

【００４４】請求項１１記載の本発明にあっては、公開鍵抽出処理においては証明書検証処理内で証明書内の認証機関の署名を検証するため、証明書に対する認証機関の証明書検証処理が実際に可能となり、証明書の有効性の有無を確認し、不当なプログラムまたはデータの利用を回避することができる。

【００４５】更に、請求項１２記載の本発明は、請求項９または１１記載の発明において、前記証明書検証処理手段が、証明書から有効期限を抽出する有効期限抽出処理手段と、前記ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と前記有効期限抽出手段で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理手段とを有することを要旨とする。

【００４６】請求項１２記載の本発明にあっては、ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行うため、証明書の有効期間の検証処理を行うことができる。

【００４７】請求項１３記載の本発明は、請求項１０または１１記載の発明において、前記データ解析手段が、前記ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離する時刻情報抽出処理手段を有し、前記証明書検証処理手段が、証明書から有効期限を抽出する有効期限抽出処理手段と、前記時刻情報抽出手段で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と前記有効期限抽出手段で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理手段を有することを要旨とする。

【００４８】請求項１３記載の本発明にあっては、ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離し、証明書から有効期限を抽出し、時刻情報抽出処理で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行うため、ＩＣカード端末から送信されたデータの中から時刻情報を抽出することができ、この時刻情報に基づいて証明書の有効期間の検証が可能となる。

【００４９】また、請求項１４記載の本発明は、請求項１１または１２または１３記載の発明において、前記証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、前記ＩＣカードが、認定済みデータ解析処理手段または有効期限抽出処理手段または証明書署名抽出処理手段から要求を受け付け、前記バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理手段を有することを要旨とする。

【００５０】請求項１４記載の本発明にあっては、証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、認定済みデータ解析処理または有効期限抽出処理または証明書署名抽出処理から要求を受け付け、バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理を行うため、従来のタグ、レングス、値の構造（以下、ＴＬＶ構造と称する）を有する例えばＸ．５０９の転送構文データをＩＣカード内で処理する場合に、高速にＩＣカード内で証明書から有効期限抽出処理または公開鍵抽出処理を行うことができる。

【００５１】更に、請求項１５記載の本発明は、請求項９乃至１４のいずれかに記載の発明において、前記コマンド制御手段が、ＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定手段と、コマンド実行手段にディスパッチする前に、前記データ署名検証制御判定手段の結果に基づき署名・証明書がある場合にデータ署名検証制御手段に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御手段とを有することを要旨とする。

【００５２】請求項１５記載の本発明にあっては、コマンド制御処理においてはＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定処理と、コマンド実行処理にディスパッチする前に、データ署名検証制御判定処理の結果に基づき署名・証明書がある場合にデータ署名検証制御処理に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御処理とを行うため、ダウンロードコマンド以外の任意のコマンドに対してコマンドの実行前にコマンドに対して入力されたデータに対して署名の検証処理を実行し、データの正当性を検証することができる。

【００５３】請求項１６記載の本発明は、請求項９乃至１５のいずれかに記載の発明において、前記データ署名検証制御手段は、前記ＩＣカード端末からの要求を受け、コマンド制御手段から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御手段に返却するデータ署名検証インタフェース手段を有し、前記公開鍵抽出処理手段は、前記ＩＣカード端末からの要求を受け、コマンド制御手段から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御手段に返却する公開鍵抽出インタフェース処理手段を有し、前記証明書検証処理手段は、前記ＩＣカード端末からの要求を受け、コマンド制御手段から証明書と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明書の正当性の検証結果をコマンド制御手段に返却する証明書検証インタフェース手段を有することを要旨とする。

【００５４】請求項１６記載の本発明にあっては、データ署名検証制御処理においてＩＣカード端末からの要求を受け、コマンド制御処理から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御に返却するデータ署名検証インタフェース処理を行い、公開鍵抽出処理においてはＩＣカード端末からの要求を受け、コマンド制御処理から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御処理に返却する公開鍵抽出インタフェース処理を行い、証明書検証処理においてはＩＣカード端末からの要求を受け、コマンド制御処理から証明書と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明　の正当性の検証結果をコマンド制御処理に返却する証明書検証インタフェース処理を行うため、例えば端末側から簡単に例えばＸ．５０９の証明書形式を有する証明書に対するＩＣカードを利用した多様な証明書処理を実施することができる。

【００５５】また、請求項１７記載の本発明は、ＩＣカードサービスサーバと、ＩＣカード端末と、該ＩＣカード端末とＩＣカードの通信を行う転送処理手段、ＩＣカード端末から送信または要求されるコマンドデータを所望のコマンド実行部にディスパッチするためのコマンド制御手段、およびコマンドを実行する複数のコマンド実行手段を有するＩＣカードとを有するＩＣカードシステムにおいてＩＣカードサービスサーバからＩＣカード端末を介してまたはＩＣカード端末からＩＣカードに送信されたデータの改竄または不正を防止するためのＩＣカードシステム通信データ保護処理プログラムを記録した記録媒体であって、ＩＣカードにおいては、ＩＣカード端末から送信されたデータ部、このデータ部を保証する人の秘密鍵を用いた署名、この署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれらの少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子

と署名を少なくとも含み、更にこの証明の有効期限を含む証明書に基づき証明書から公開鍵を抽出する公開鍵抽出処理と、この抽出された公開鍵に基づいて署名検証処理を実行するデータ署名検証処理を少なくとも有するデータ署名検証制御処理とを行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００５６】請求項１７記載の本発明にあっては、証明書から公開鍵を抽出し、この抽出された公開鍵に基づいて署名検証処理を実行するため、プログラムまたはデータに対する署名検証をＩＣカード内で実施することができ、また公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書形式を処理するため、既存に流通している証明書と整合性の高い署名検証処理が可能となり、また認証機関の署名と証明書有効期間が設定されているＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００５７】更に、請求項１８記載の本発明は、請求項１７記載の発明において、データ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明　部で少なくとも構成される認定済みデータが前記ＩＣカード端末からＩＣカードに送信され、前記データ署名検証制御処理においては、ＩＣカード端末から送信されたデータ部と、このデータ部を保証する人の秘密鍵を用いた署名部と、署名に用いた秘密鍵に対する公開鍵の証明を行うものであって、公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出処理、署名部抽出処理、および証明書抽出処理で構成される認定済みデータ解析処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００５８】請求項１８記載の本発明にあっては、データ署名検証制御処理において公開鍵の所有者の識別子とデータ部署名者の公開鍵とこれら少なくとも前記識別子と公開鍵情報を保証する認証機関の識別子と署名を少なくとも含み、更にこの証明の有効期限を含む証明書部で少なくとも構成される認定済みデータの解析を行うデータ抽出処理、署名部抽出処理および証明書抽出処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００５９】請求項１９記載の本発明は、請求項１７または１８記載の発明において、前記公開鍵抽出処理においては、証明書検証処理内に証明書内の認証機関の署名を検証する証明書署名検証処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００６０】請求項１９記載の本発明にあっては、公開鍵抽出処理においては証明書検証処理内で証明書内の認証機関の署名を検証するＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００６１】また、請求項２０記載の本発明は、請求項１７または１９記載の発明において、前記データ解析処理においてはＩＣカード端末から付加的な要素として送信された時刻に基づき、前記証明書検証処理において証明書から有効期限を抽出する有効期限抽出処理と、前記ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理とを行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００６２】請求項２０記載の本発明にあっては、ＩＣカード端末から送信された時刻情報または時刻管理が可能なＩＣカード内で管理された時刻情報と有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００６３】更に、請求項２１記載の本発明は、請求項１８または１９記載の発明において、前記データ解析処理においては、前記ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離する時刻情報抽出処理を行い、前記証明書検証処理においては、証明書から有効期限を抽出する有効期限抽出処理と、前記時刻情報抽出処理で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と前記有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行う有効期限検証処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００６４】請求項２１記載の本発明にあっては、ＩＣカード端末から付加的な要素として送信された時刻である時刻情報部を他の認定済みデータから分離し、証明書から有効期限を抽出し、時刻情報抽出処理で得られた時刻情報または時刻管理が可能なＩＣカード内部で管理された時刻情報と有効期限抽出処理で得られた有効期限との比較を行い、証明書有効期限の検証を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記

録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００６５】請求項２２記載の本発明は、請求項１９または２０または２１記載の発明において、前記証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、前記ＩＣカードにおいては、前記認定済みデータ解析処理または前記有効期限抽出処理または証明書署名抽出処理から要求を受け付け、前記バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００６６】請求項２２記載の本発明にあっては、証明書部の構造が階層化されたタグと長さと値で表現されたバイナリデータであって、認定済みデータ解析処理または有効期限抽出処理または証明書署名抽出処理から要求を受け付け、バイナリデータをタグ・長さ・値のまま処理を行い、必要なタグの値のみ抽出するタグ・レングス・値バイナリ構文解析処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録しているため、該記録媒体を用い、その流通性を高めることができる。

【００６７】また、請求項２３記載の本発明は、請求項１７乃至２２のいずれかに記載の発明において、前記コマンド制御処理においては、ＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定処理と、コマンド実行処理にディスパッチする前に、前記データ署名検証制御判定処理の結果に基づき署名・証明書がある場合にデータ署名検証制御処理に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御処理とを行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００６８】請求項２３記載の本発明にあっては、コマンド制御処理においてはＩＣカードから送信された任意のコマンドのデータ部に対する署名と証明書の有無を判定するデータ署名検証制御判定処理と、コマンド実行処理にディスパッチする前に、データ署名検証制御判定処理の結果に基づき署名・証明書がある場合にデータ署名検証制御処理に対して該データに対する署名正当性の検証を行うためのデータの受け渡しを行うデータ署名検証制御処理とを行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００６９】更に、請求項２４記載の本発明は、請求項１７乃至２３のいずれかに記載の発明において、前記データ署名検証制御処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御処理に返却するデータ署名検証インタフェース処理を行い、前記公開鍵抽出処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御処理に返却する公開鍵抽出インタフェース処理を行い、前記証明書検証処理においては、前記ＩＣカード端末からの要求を受け、コマンド制御処理から証明書と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明書の正当性の検証結果をコマンド制御処理に返却する証明書検証インタフェース処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録することを要旨とする。

【００７０】請求項２４記載の本発明にあっては、データ署名検証制御処理においてＩＣカード端末からの要求を受け、コマンド制御処理から認定済みデータと付加的に時刻情報を受け取り、署名の正当性の検証結果をコマンド制御に返却するデータ署名検証インタフェース処理を行い、公開鍵抽出処理においてはＩＣカード端末からの要求を受け、コマンド制御処理から証明書と付加的に時刻情報を受け取り、証明書から抽出された公開鍵を少なくとも有する証明書内のデータをコマンド制御処理に返却する公開鍵抽出インタフェース処理を行い、証明書検証処理においてはＩＣカード端末からの要求を受け、コマンド制御処理から証明　と証明書に対する署名の公開鍵番号と付加的に時刻情報を受け取り、証明書の正当性の検証結果をコマンド制御処理に返却する証明　検証インタフェース処理を行うＩＣカードシステム通信データ保護処理プログラムを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【００７１】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。図１は、本発明の一実施形態に係るＩＣカードシステム通信データ保護処理方法を実施するＩＣカードシステムの構成を示すブロック図である。図１に示すＩＣカードシステムは、ＩＣカード端末４－１およびＩＣカード４－２から構成され、ＩＣカード４－２は転送処理部４－３、コマンド制御部４－４、データ署名検証制御部４－７、コマンド実行処理部４－８、公開鍵抽出処理部４－９、証明書検証処理部４－２２、公開鍵形式変換処理部４－１１、証明書署名者公開鍵４－３３の接続された署名検証処理部４－１２、ＴＬＶ構文解析処理部４－１８から構成されている。

【００７２】また、コマンド制御部４－４は、データ署名検証制御判定部４－５、データ署名検証制御要求部４－６から構成され、データ署名検証制御部４－７は、データ署名検証インタフェース部４－３１、認定済みデータ解析処理部４－１３、公開鍵抽出制御部４－１９、公開鍵形式変換制御部４－２９、データ署名検証処理部４

－３０から構成され、認定済みデータ解析処理部４－１３は、データ部抽出部４－１４、署名部抽出部４－１５、証明書抽出部４－１６、時刻情報部抽出部４－１７から構成されている。更に、公開鍵抽出処理部４－９は、公開鍵抽出インタフェース処理部４－２０、証明書検証制御部４－２１、公開鍵抽出処理実行部４－２８から構成されている。証明書検証処理部４－２２は、証明書検証インタフェース処理部４－２３、有効期限抽出処理部４－２４、有効期限検証処理部４－２５、証明書署名抽出処理部４－２６、証明書署名検証処理実行部４－２７から構成されている。

【００７３】次に、上述したように構成される実施形態の作用について図２に示すフローチャートおよび図３に示すＩＣカード通信データ構造を参照して説明する。

【００７４】まず、ＩＣカード端末４－１より、認定済みデータとして、ＴＬＶ構造をもつデータ・署名・証明書の対が送信され、時刻情報がこの認定済みデータの後にＴＬＶ構造で添付されているとする（図３のＣＡＳＥ２）。このとき、ＩＣカード４－２内の転送処理部４－３はこの情報をＩＣカード端末４－１からＩＣカード４－２内のコマンド制御部４－４へと転送を実施し、コマンド制御部４－４にコマンドデータを渡す。コマンド制御部４－４では、データ署名検証制御の判定を行うような設定がＩＣカード内あるいはＩＣカード内のコマンドが指定された領域内あるいはコマンド単位でなされている場合には、データ署名検証制御判定部４－５において、認定済みデータのタグを見つけた場合に署名検証が必要であると判断し、認定済みデータ＋時刻情報をデータ署名検証制御要求部４－６に転送する。データ署名検証制御要求部４－６ではこの情報をデータ署名検証制御部４－７に転送する。

【００７５】もし、認定済みデータのタグがなかった場合には、コマンドを通常と同様に指定されたコマンドに対するコマンド実行処理部４－８に渡す（このコマンド実行処理部４－８は、データ署名検証制御部４－７、公開鍵抽出処理部４－９、証明書検証処理部４－２２、公開鍵形式変換処理部４－１１、署名検証処理部４－１２を含む。このときそれぞれの、インタフェース処理部がコマンド制御部４－４とのインタフェースを受け持つ。個々の説明は後述する）。なお、このデータ署名検証制御判定方法は多様な設定が考えられる（例えば、シンプルＴＬＶ（階層を持たないＴＬＶデータの列）構造で、最後に署名＋証明書＋時刻情報（オプション）があった場合は、プロトコルヘッダから署名までをデータとみなすかあるいはプロトコルヘッダから署名までをデータとみなしてデータ署名検証制御を行う等など）。また、コマンド制御部４－４はデータ署名検証制御判定部４－５を持たず、すべてのコマンドをコマンド実行処理部にディスパッチし、コマンド実行処理部においてデータ署名検証制御部４－７に認定済みデータ＋時刻情報の形式で（コマンド実行部にデータ＋署名＋証明書＋時刻情報などのような形式で渡っている場合は認定済みデータ＋時刻情報の形式に組み立て直して送信する。他に双方で形式の共通理解があればよい）情報を渡して、データ署名検証制御を実施してもよい。

【００７６】次に、データ署名検証制御部４－７の処理フローを説明する。データ署名検証制御部４－７では、データ署名検証インタフェース部４－３１で認定済みデータ＋時刻情報を受け取り、認定済みデータ解析処理部４－１３に処理を依頼する。認定済みデータ解析処理部４－１３では、認定済みデータ（前述のように、データ署名検証制御主要部に渡される形式は、双方の共通理解があればよい。例えば、データ＋署名＋証明書＋時刻情報のようであってもよい）の構造解析を行う。ＴＬＶ構造を判定し、データ部抽出部４－１４においてデータの抽出を行い、署名部抽出部４－１５において署名の抽出を行い、証明書抽出部４－１６において証明書の抽出を行い、時刻情報部抽出部４－１７において時刻情報の抽出を行う。なお、構造の解析と値の抽出にあたっては、ＴＬＶ構文解析処理部４－１８の解析ルーチン（例えばタグ番号入力に対して値を返すなど共通的なルーチンを利用するものから、特定の解析ルーチンを複数用意して、これを利用するなど）を利用して処理を実施してもよい。なお、解析されたデータはメモリ上におくかあるいはファイルに書き込み処理を利用して書き込んでおき（特に、データは大きいのでデータだけはファイルに書き出すとか）、終了後に消去する。

【００７７】次に、証明書からの公開鍵の抽出処理について説明する。公開鍵の抽出処理はデータ署名検証制御部４－７の公開鍵抽出制御部４－１９がＩＣカード内の公開鍵抽出処理部４－９に対して、処理要求として証明書を送信するところから開始される。公開鍵抽出処理部４－９は、公開鍵抽出インタフェース処理部４－２０を介して、公開鍵抽出処理制御部４－１９から処理依頼を受け、これを証明書検証制御部４－２１に渡す。証明書検証制御部４－２１は、ＩＣカード内の証明書検証処理部４－２２ではまず、証明書検証インタフェース処理部４－２３が証明書と時刻情報を受け取り、有効期限抽出処理部４－２４に渡す。有効期限抽出処理部４－２４では証明書から有効期限のみ値を抽出し、この値を有効期限検証処理部４－２５に渡す。なお、有効期限抽出処理部４－２５はこの値の抽出にあたって、このモジュールにてＴＬＶ構造の解析を実施してもよいが、前記認定済みデータ解析処理部４－１３が実施したようにＴＬＶ構文解析処理裡部４－１８を利用してもよい。有効期限検証処理部４－２５では、メモリ上あるいはファイル内（あるいは公開鍵抽出制御部４－１９から公開鍵抽出処理部４－９に渡された）時刻情報、あるいは時刻情報管理機能を有するＩＣカードにおいては、得られた時刻情報を利用して、渡された有効期限を時刻情報が満たしているかどうかの判定を行う。もし、時刻情報を満たしていない場合には公開鍵抽出制御部４－９に対してエラーを返却する。もし、満たしている場合は、証明書署名抽出処理部４－２６に証明書を渡す。証明書署名抽出処理部４－２６では、証明書に署名された認証期間の署名の抽出を実施するが、これは前記有効期限抽出処理４－２４と同様にＴＬＶ構文解析処理部４－１８を利用して署名の抽出を行ってもよい。署名の抽出が終了後、証明書署名検証処理実行部４－２７において、証明書の署名に対する検証を実施する。このとき、例えば、認証期間の公開鍵データは予めＩＣカード内の鍵データとして格納しておき、コマンドのパラメータの１つとしてこの鍵データの識別を指定するようにする。証明書署名検証処理実行部４－２７は、ＩＣカード内の署名検証処理部４－１２に処理を依頼し、署名検証処理部４－１２は証明書のデータと署名データ、および該公開鍵データの鍵識別子を利用して署名の検証を実施する。もし署名が正しくない場合には公開鍵抽出制御部４－１９にエラーを返却する。正しい場合には、公開鍵抽出処理実行部４－２８に証明書を渡し、証明書から公開鍵の抽出を実施する。公開鍵抽出処理実行部４－２８によるＴＬＶ構文の解析方法については前述の通りである。抽出が成功した場合には、抽出した公開鍵を公開鍵抽出制御部４－１９に返却する。

【００７８】次に、公開鍵抽出制御部４－１９が受け取った公開鍵が署名検証処理部４－１２の処理できる形式でない場合に、公開鍵形式変換制御部４－２９に公開鍵を渡す。公開鍵形式変換制御部４－２９は公開鍵形式変換処理部４－１１に公開鍵を渡し、公開鍵の所望の形式への変換を実施する。

【００７９】最後に変換された公開鍵を元に、データ署名検証処理部４－３０がＩＣカードより送信されたデータに対する署名の検証を署名検証処理部４－１２に依頼することによって、すべてのデータ検証作業を終了する。

【００８０】なお、データ署名検証制御部４－７、公開鍵抽出処理部４－９、証明書検証処理部４－２２以外で、公開鍵形式変換処理部４－１１、署名検証処理部４－１２等を含むすべてのコマンド実行処理部４－８はすべてインタフェース処理部を有し、ＩＣカード端末あるいはＩＣカード内の他のコマンド実行処理部４－８から依頼された処理を実行するインタフェースを提供する。

【００８１】また、公開鍵抽出処理部はオプションとして、公開鍵の他にオプションとして、公開鍵の所有者の識別子などの情報を出力する。

【００８２】なお、図３において、ＣＡＳＥ１、すなわちＭｕｌｔｏｓのようにデータ、署名、証明書を別々に送信する際には、例えば任意のコマンドについて、データ部で設定する情報を予め送信しておき、最後にコマンドを実施するというような方式となる。このとき、データ、署名、証明書はコマンド用の共通メモリエリアあるいはファイルにテンポラリデータとして保持されなければならない。

【００８３】なお、上記実施形態の処理をプログラムとして記録媒体に記録することにより該記録媒体を用いて、その流通性を高めることができる。

【００８４】

【発明の効果】以上説明したように、本発明によれば、（１）ＩＣカードサービスサーバ、ＩＣカード端末、ＩＣカードを含む分散環境において、エンドユーザ（任意のサービスプロバイダを含む）によって既存の署名・証明書管理環境を用いた容易なデータ保証を行うことができ、かつこのデータをエンドユーザ間で流通させることが可能となる。

【００８５】また、本発明によれば、（２）既存に流通している証明書と整合性の高い署名検証処理が可能となり、また認証機関の署名と証明書有効期間が設定されているので、この情報を利用すれば証明書を流通させても改竄の恐れがなく、また証明書が有効でない場合に利用するというような危険性を回避することが可能となる。

【００８６】更に、本発明によれば、（３）証明書に対する認証機関の署名を検証することが可能となるので、分散環境で署名＋証明書付きのデータ（プログラムを含む）を安全に流通させることが可能となり、これにより分散ＩＣカードシステム環境においてエンドユーザ間で相互にデータやプログラムを交換する環境が提供できる。

【００８７】本発明によれば、（４）データ・署名・証明書が一体となったデータ（ファイル）として任意のデータが管理可能であるので、分散環境において署名・証明書付きデータを流通させた場合に、個々に管理する方法に比較して、紛失などの管理上の混乱を回避することが可能となるほか、個々の処理の容易性も確保できる。

【００８８】また、本発明によれば、（５）証明書の有効期間の検証処理が可能となるので、証明書を複数の管理機関で管理し、また既存の証明書管理機関で発行されたＸ．５０９のような証明書を利用することが可能となり、ＩＣカードのデータ保証を行うための仕組みとして、安全性を保証したまま、より柔軟な公開鍵の管理、すなわち利用者の管理が可能となる。また、これに応じて安全に署名・証明書付きデータを分散環境で流通させることが可能である。

【００８９】更に、本発明によれば、（６）上述した（３）のようなデータ・署名・証明書一体型のデータの流通環境においても上記（５）のように証明書の有効期間の検証が可能となるので、データの管理の容易性を確保したまま安全な分散流通を図ることが可能である。

【００９０】本発明によれば、（７）従来のタグ・レングス・値の構造（以下、ＴＬＶ構造）をもつ例えばＸ．５０９の転送構文データをＩＣカード内で処理する場合

に、高速にＩＣカード内で証明書から有効期限抽出処理あるいは公開鍵抽出処理を行うことが可能となる。

【００９１】また、本発明によれば、（８）ダウンロードコマンド以外の任意のコマンドに対して、コマンドを実行する前に、コマンドに対して入力されたデータに対する署名の検証処理を実行し、データの正当性を検証することが可能となる。これにより、例えばＩＳＯ７８１６－４に規定されるようなコマンドヘッダ情報＋コマンドパラメータ＋コマンドデータ部に対する署名と証明書を施し、この正当性を常にチェックすることが可能となり、コマンド送信者を保証する仕組みを提供することができる。ＩＳＯ以外のコマンドに対しては同様である。

【００９２】更に、本発明によれば、（９）個々の証明処理インタフェースをコマンド制御向けに提供することにより、ＩＣカード端末（およびＩＣカード端末を介したＩＣカードサービスサーバ）あるいはＩＣカード内の任意の他のコマンドから証明書処理インタフェースを利用することが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るＩＣカードシステム通信データ保護処理方法を実施するＩＣカードシステムの構成を示すブロック図である。

【図２】図１に示す実施形態の作用を示すフローチャートである。

【図３】図１に示す実施形態におけるＩＣカード通信データ構造を示す図である。

【図４】従来のＩＣカードシステム通信データ保護処理方法を実施する装置構成を示すブロック図である。

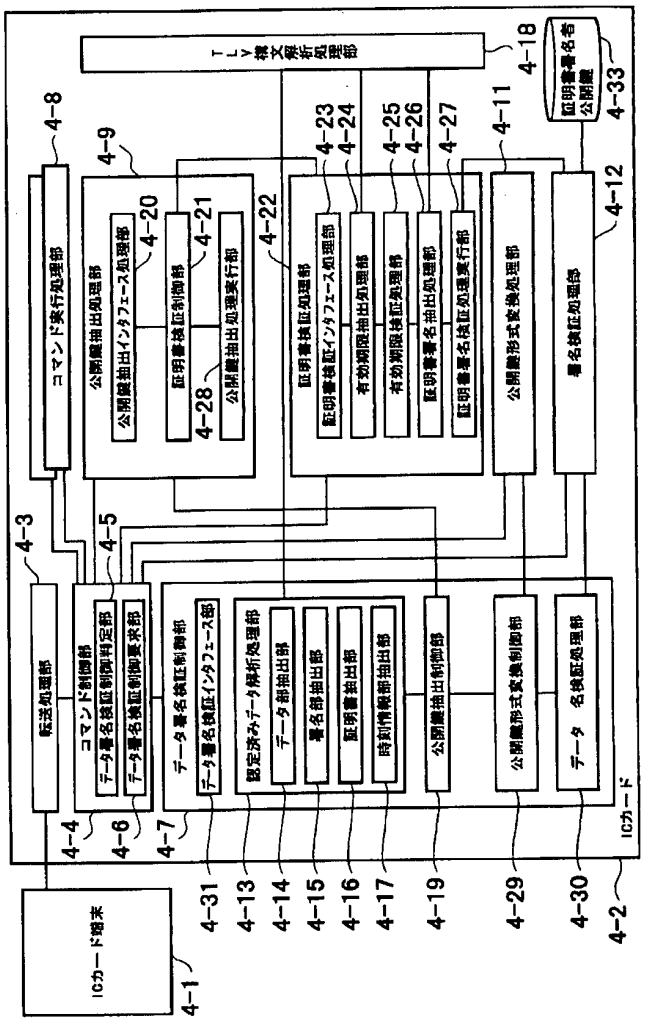
【図５】図４に示す従来のＩＣカードシステム通信データ保護処理手順を示すフローチャートである。

【図６】従来のＩＣカード通信データ構造を示す図である。

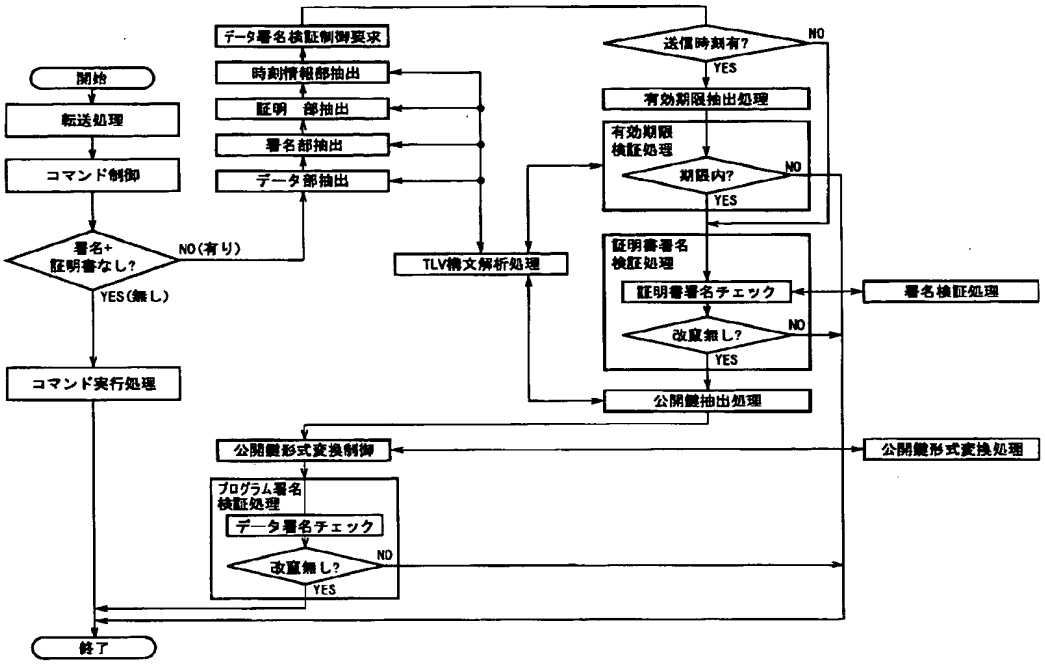
【符号の説明】

４－１　ＩＣカード端末
４－２　ＩＣカード
４－３　転送処理部
４－４　コマンド制御部
４－５　データ署名検証制御判定部
４－６　データ署名検証制御要求部
４－７　データ署名検証制御部
４－８　コマンド実行処理部
４－９　公開鍵抽出処理部
４－１１　公開鍵形式変換処理部
４－１２　署名検証処理部
４－１３　認定済みデータ解析処理部
４－１４　データ部抽出部
４－１５　署名部抽出部
４－１６　証明書抽出部
４－１７　時刻情報部抽出部
４－１８　ＴＬＶ構文解析処理部
４－１９　公開鍵抽出制御部
４－２０　公開鍵抽出インタフェース処理部
４－２１　証明書検証制御部
４－２２　証明書検証処理部
４－２３　証明書検証インタフェース処理部
４－２４　有効期限抽出処理部
４－２５　有効期限検証処理部
４－２６　証明書署名抽出処理部
４－２７　証明書署名検証処理部
４－２８　公開鍵抽出処理実行部
４－２９　公開鍵形式変換制御部
４－３０　データ署名検証処理部
４－３１　データ署名検証インタフェース部

【図１】



【図２】



【図３】

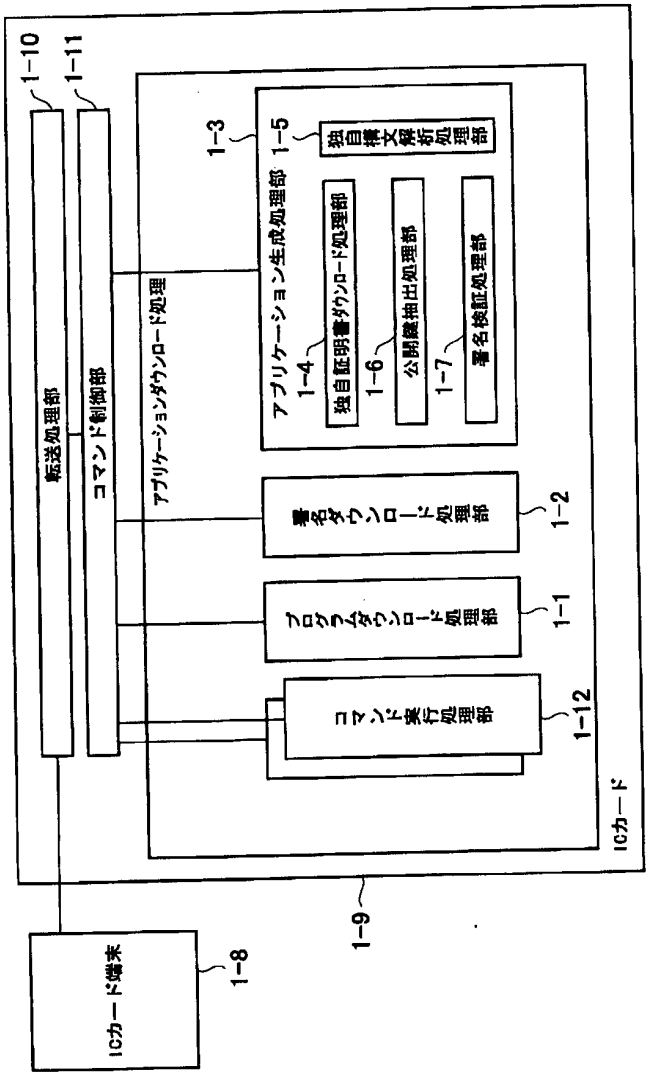
(a) CASE1：別々に送信する場合

データダウンロードコマンド	プロトコルヘッダ	データ
署名ダウンロードコマンド	プロトコルヘッダ	署名
証明書ダウンロードコマンド	プロトコルヘッダ	証明書
任意コマンド	プロトコルヘッダ	時刻情報

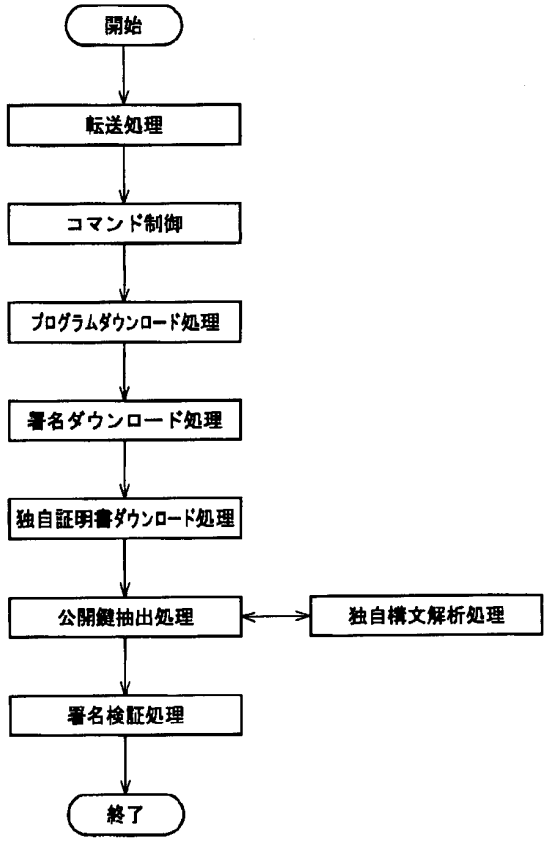
(b) CASE2：一体で送信する場合

任意コマンド	プロトコルヘッダ	認定済みデータ			時刻情報
		データ	署名	証明	
任意コマンド	プロトコルヘッダ	データ	署名	証明	時刻情報

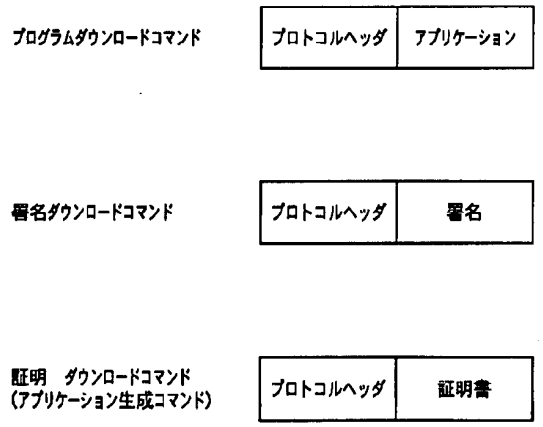
【図4】


1-10
1-11
1-3
1-5
独自構文解析処理部
アプリケーション生成処理部
1-4
独自証明書ダウンロード処理部
1-6
公開鍵抽出処理部
1-7
署名検証処理部
転送処理部
コマンド制御部
アプリケーションダウンロード処理
署名ダウンロード処理部
1-2
プログラムダウンロード処理部
1-1
コマンド実行処理部
1-12
ICカード
1-9
ICカード端末
1-8

【図5】


開始
転送処理
コマンド制御
プログラムダウンロード処理
署名ダウンロード処理
独自証明書ダウンロード処理
公開鍵抽出処理
独自構文解析処理
署名検証処理
終了

【図６】



フロントページの続き

(72)発明者　千葉　伸浩
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

(72)発明者　細田　泰弘
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B035 AA13 BB09 CA38
5B058 CA28 KA31 KA35
5J104 AA09 AA11 LA03 LA06 NA02
NA05 NA27 NA35 PA07